Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

A QSA led assessment of compliance validation according to the Payment Card Industry Data Security Standards and Security Assessment Procedures version 3.2.1.

Level 1 Service Provider Validation: According to the service provider validation requirements defined by the payment brands (including VISA, MasterCard, JCB, American Express and Discover) in PCI industry, the annual onsite review by QSA for level 1 service provider could be compulsory.

Alibaba Cloud (Singapore) Private Limited
For Security Services Products

Report Date: July 17, 2019
Initial Compliance Date: July 14, 2018
Report Number: C131-36-2019-B
The assessment remains valid for 12 months

atsec (Beijing) Information Technology Co., Ltd
3/F, Block C, Bld.1, Boya C-Center, Life Science Park
Tel: +86 10 53056679
Fax: +86 10 53056678
http://www.atsec.cn

The attestation of compliance is based on the template (version 3.2.1, June 2018) copyrighted by PCI Security Standards Council LLC

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	Alibaba Cloud (Singapore) Private Limited (Branded as "Alibaba Cloud")		DBA (doing business as):	N/A	
Contact Name:	Larry Liu		Title:	Head of Security and Privacy Compliance	
Telephone:	+65 68307260		E-mail:	larry.ly@alibaba-inc.com	
Business Address:	8 Shenton Way #45-01, AXA Tower		City:	Singapore	
State/Province:	-	Country:	Singapore	Zip:	068811
URL:	https://www.alibabacloud.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	atsec (Beijing) Information Technology Co., Ltd				
Lead QSA Contact Name:	Jinyun Chen		Title:	QSA, Principal Consultant	
Telephone:	+86 10 5305 6679		E-mail:	jinyun@atsec.com	
Business Address:	3/F, Block C, Bld.1, Boya C-Center, Life Science Park		City:	Beijing	
State/Province:	-	Country:	P.R. China	Zip:	102206
URL:	https://www.atsec.com				

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2. Executive Summary		
Part 2a. Scope Verification		
Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) assessed:	Action Trail, Anti-Bot, Anti-DDoS Premium, Billing System, Server Guard, Threat Detection Service (Hereinafter referred to as "TDS"), and Web Application Firewall (Hereinafter referred to as “WAF”)	
Type of service(s) assessed:		
Hosting Provider: ☒ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☒ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☒ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		
***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity’s service description. If you feel these categories don’t apply to your service, complete “Others.” If you’re unsure whether a category could apply to your service, consult with the applicable payment brand.*		

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) not assessed:	All other services provided by Alibaba Cloud are not included in the scope of PCI DSS assessment (except Action Trail, Anti-Bot, Anti-DDoS Premium, Billing System, Server Guard, TDS, and WAF)	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:	Based on business decision from Alibaba Cloud, services except Action Trail, Anti-Bot, Anti-DDoS Premium, Billing System, Server Guard, TDS, and WAF service were excluded from this PCI DSS assessment.	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Action Trail, Anti-Bot, Anti-DDoS Premium, Server Guard, TDS and WAF themselves do not directly transmit, process, or store cardholder data, and the PCI compliant environment facilitates its clients' PCI DSS compliance (i.e. that the products or systems do not enforce implementation or configuration settings that violates a PCI DSS requirement). Public Cloud International Services of Alibaba Cloud provides card-not-present payment method for its clients to purchase service on Alibaba Cloud webpage. Once the purchasing order has been created, the cardholder data (PAN, Cardholder Name and Expiration date) and sensitive authentication data (CVV2/CVC2/CID) are input on the web page of Alibaba Cloud Billing System, then these information are transmitted to Alibaba Cloud Billing System by using strong cryptography over Internet. Once Alibaba Cloud Billing System complete internal processing, the cardholder data and sensitive authentication data are then forwarded to payment processor (Alipay Labs (Singapore) Pte. Ltd.) over Internet with strong cryptography. Cardholder data (PAN, Cardholder Name and Expiration date) and sensitive authentication data (CVV2/CVC2/CID) are held in the VRAM (Volatile Random Access Memory) and purged immediately after authorization. No cardholder data and sensitive authentication data are stored in the Alibaba Cloud environment.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	All Alibaba Cloud system components are hardened according to identical security baselines and managed under the same vulnerability and patch management policies. The cloud services excluded from the scope of this QSA assessment are put in different zone of the clusters and separated via strict access controls. The access controls are enforced by the core switch within Alibaba Cloud production environment.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2c. Locations		
List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.		
Type of facility:	**Number of facilities of this type**	**Location(s) of facility (city, country):**
Office Network	2	Hangzhou Office is located in Apsara Park, Shilongshan Road, Xihu District, Hangzhou City, Zhejiang Province, P.R.China, 310024 Singapore Office is located in 8 Shenton Way #45-01, AXA Tower, Singapore, 068811.
Datacenter	29	**Cloud Datacenters:** ■ Hong Kong Zone B ■ Hong Kong Zone C ■ Asia Pacific SE 1 (Singapore) Zone A ■ Asia Pacific SE 1 (Singapore) Zone B ■ Asia Pacific SE 1 (Singapore) Zone C ■ Asia Pacific SE 2 (Sydney) Zone A ■ Asia Pacific SE 2 (Sydney) Zone B ■ Asia Pacific SE 3 (Kuala Lumpur) Zone A ■ Asia Pacific SE 3 (Kuala Lumpur) Zone B ■ Asia Pacific SE 5 (Jakarta) Zone A ■ Asia Pacific SE5 (Jakarta) Zone B ■ Asia Pacific SOU 1(Mumbai) Zone A ■ Asia Pacific SOU1 (Mumbai) Zone B ■ EU Central 1 (Frankfurt) Zone A ■ EU Central 1 (Frankfurt) Zone B ■ Middle East 1 (Dubai) Zone A ■ US East 1 (Virginia) Zone A ■ US East 1 (Virginia) Zone B ■ US West 1 (Silicon Valley) Zone A ■ US West 1 (Silicon Valley) Zone B ■ UK London Zone A ■ UK London Zone B **Anti-DDoS Premium Datacenters:** ■ JP141 Site-Data Processing Zone ■ OE24 Site-Data Processing Zone ■ OE26 Site-Data Processing Zone ■ OE28 Site-Data Processing Zone ■ OI39 Site-Data Processing Zone ■ MY86 Site-Data Processing Zone ■ US50 Site-Data Processing Zone *Note: The detail location of above datacentres are removed based on Alibaba Cloud's confidential requirement. The detail addresses of those datacentres are recorded in the ROC which release by atsec (Beijing) information Technology Co., Ltd at July 17, 2019.*

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2d. Payment Applications
Does the organization use one or more Payment Applications? ☒ Yes ☐ No
Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Bill System	20190422	Alibaba Cloud	☐ Yes ☑ No	Not applicable.

Part 2e. Description of Environment	
Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	All system components of this PCI DSS QSA assessment are located in above datacenters. The critical system components involved in this QSA scope include Action Trail, Anti-Bot, Anti-DDoS Premium, Billing System, Server Guard, TDS and WAF Service related servers, Billing system, bastion machine, and NTP server. Only the security of cloud infrastructure and related administration security mechanisms are covered in this PCI DSS assessment.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	Not applicable.
QIR Individual Name:	Not applicable.
Description of services provided by QIR:	Not applicable.
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No
If Yes:	
Name of service provider:	**Description of services provided:**
Alipay Labs (Singapore) Pte. Ltd.	Payment authorization service.
Note: *Requirement 12.8 applies to all entities in this list.*	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website*.

Name of Service Assessed:	Anti-Bot, Anti-DDoS Premium, Billing System, Server Guard, TDS and WAF Service			
	Details of Requirements Assessed			
PCI DSS Requirement	**Full**	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	Requirement 1.2.3 was marked as not applicable. Because wireless networks are not enabled in the scope of this PCI DSS assessment. Requirement 1.3.6 was marked as not applicable. Because cardholder data are not stored in cardholder data environment.
Requirement 2:	☐	☒	☐	Requirement 2.1.1 was marked as not applicable. Because wireless networks are not enabled in the scope of this PCI DSS assessment. Requirement 2.6 was marked as not applicable. Because the in-scope Anti-Bot, Anti-DDoS Premium, Billing System, Server Guard, TDS and WAF Service are not shared hosting service and no shared hosting service are involved in this PCI DSS assessment.
Requirement 3:	☐	☒	☐	Requirements 3.1 and 3.4 were marked as not applicable. Because cardholder data are not stored in the cardholder data environment. Requirement 3.3 was marked as not applicable. Because full PANs or mask PANs are not visible to internal personnel. Requirement 3.4.1 was marked as not applicable. Because disk level encryption mechanisms are not engaged for the cardholder data protection. Requirements 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7 and 3.6.8 were marked as not applicable. Because cardholder data are not stored in the cardholder

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

				data environment and thus encryption keys are not used to protect cardholder data.
Requirement 4:	☐	☒	☐	Requirement 4.1.1 was marked as not applicable. Because wireless networks are not enabled in the scope of this PCI DSS assessment. Requirement 4.2 was marked as not applicable. Because PANs are not transmitted via end-user messaging technologies.
Requirement 5:	☒	☐	☐	All requirements in this section were marked as applicable.
Requirement 6:	☒	☐	☐	All requirements in this section were marked as applicable.
Requirement 7:	☒	☐	☐	All requirements in this section were marked as applicable.
Requirement 8:	☐	☒	☐	Requirement 8.1.5 was marked as not applicable. Because vendor accounts are not enabled in the cardholder data environment. Requirement 8.7 was marked as not applicable. Because cardholder data are not stored in database servers.
Requirement 9:	☐	☒	☐	Requirements 9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1 and 9.8.2 were marked as not applicable. Because media is not engaged in the storage of cardholder data. Requirements 9.9, 9.9.1, 9.9.2 and 9.9.3 were marked as not applicable. Because card-present services are not supported in the cardholder data environment.
Requirement 10:	☐	☒	☐	Requirement 10.2.1 was marked as not applicable. Because cardholder data are not stored in database servers or in cardholder data environment.
Requirement 11:	☐	☒	☐	Requirement 11.1.1 was marked as not applicable. Because wireless access points are not enabled in the cardholder data environment.
Requirement 12:	☐	☒	☐	Requirement 12.8.5 was marked as not applicable. Because PCI DSS requirements are not managed by external entities.
Appendix A1:	☐	☐	☒	All requirements were marked as not applicable. Because the in-scope Anti-Bot, Anti-DDoS Premium, Billing System, Server Guard, TDS and WAF Service are not shared hosting service and no shared hosting service are involved in this PCI DSS assessment.
Appendix A2:	☐	☒	☐	Requirement A2.1 was marked as not applicable. Because POS POI terminals are not supported in the scope of this PCI DSS assessment.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	July 17, 2019
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes ☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements not tested?	☐ Yes ☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *July 17, 2019***.**

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Alibaba Cloud (Singapore) Private Limited* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *Alibaba Cloud (Singapore) Private Limited* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *atsec (Beijing) Information Technology Co., Ltd*

Part 3b. Service Provider Attestation	
Signature of Service Provider Executive Officer ↑	*Date: July 17, 2019*
Service Provider Executive Officer Name: Larry Liu (刘洋)	*Title: Head of Security and Privacy Compliance*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	QSA assessment and evidence validation.

Signature of Duly Authorized Officer of QSA Company ↑	*Date: July 17, 2019*
Duly Authorized Officer Name: Jinyun Chen (陈谨运)	*QSA Company: atsec (Beijing) Information Technology Co., Ltd*

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)	
If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Not applicable. Because ISA is not involved in this PCI DSS assessment.

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections	☒	☐	

---------- The end of the document ----------

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.